IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	**)**	
	)	
v.	**)**	**Case No. 22-cr-136**
	)	
ALEXEY RENE GAVINO	**)**	
	)	
	)	

ALEXEY GAVINO'S POST HEARING SUPPLEMENTAL BRIEF IN SUPPORT OF MOTION TO SUPPRESS

Alexey Rene Gavino moved to suppress all evidence against him obtained as the result of the unlawful search of his iPhone. *See* ECF No. 22. The government in their opposition papers raised questions of fact regarding whether Mr. Gavino was "compelled" to provide his passcode and whether or not he was in "custody" at the time he was forced to provide the passcode. *See* ECF No. 25 at 7-12. However, the testimony at the hearing[1], demonstrates that Mr. Gavino was, in fact, compelled to provide his passcode while in custody. Additionally, the testimony at the hearing and a recent decision from the Southern District of New York demonstrate that a warrant, or, at minimum, reasonable suspicion, was required to conduct a manual search of Mr. Gavino's electronic device, and that the good faith doctrine does not apply.

HEARING SUMMARY

On August 30, 2021, law enforcement conducted a three-and-a-half-hour search of Mr. Gavino, his physical property, and the contents of his iPhone. Tr. 68:23-69:6. This search was predicated on a "one day lookout" because the government purportedly seized $37,000 from Mr. Gavino while he traveled on a domestic flight to LAX in 2019. Tr. 24: 19-25:8. No drugs were

[1] A hearing on the motion to suppress was held on August 14, 2023. The government called one witness - Customs and Border Patrol ("CBP") Officer Joseph Sottile.

recovered from Mr. Gavino during that stop, and he was never arrested or charged with a crime. Tr. 39:13-18. As far as Officer Sottile remembered nothing suspicious happened between 2019 and August 2021. Tr. 41:2-10. Finally, the "lookout" did not include any information about Mr. Gavino's travels on August 30, 2021, other than the fact he was coming from the Dominican Republic to New York.

This "lookout" caused Mr. Gavino to be processed through a secondary inspection. Officer Sottile testified that the purpose of a secondary inspection is to "to examine the person that travels, what they stated they went there for and to conclude that it was legitimate travel, you have a legitimate traveler in front of you." Tr. 10:9-12; *see also* Tr. 7:2-6. Officers are are supposed to "ask [travelers] about their bags, if its's theirs, they packed it." Tr. 10:22-24. They are supposed to search luggage to "make sure [no contraband] comes into this country" and that their luggage "matches" their travel. Tr. 10:13-17; *see also* Tr. 18:1-7. He explained "[s]ome people say they're going for a wedding, you're going to look for a dress, a suit. Something that matches their travels. If they're going for vacation, they're going to the beach, you're going to look for swimming trunks and T-shirts. Generally it's to match what they're saying they traveled for." Tr. 18:1-7.

After reading the information in the "lookout" Officer Sottile stopped Mr. Gavino outside of the primary inspection area and introduced himself as a CBP officer while wearing a visible CBP badge. Tr. 26:13-27:15. He then escorted Mr. Gavino to do a secondary exam. *Id.*; *see also* Tr. 43:7-8. At that point Mr. Gavino was not free to leave. Tr. 43:9-11. Officer Sottile walked Mr. Gavino away from the exit where all of the other travelers were going, through a set of metal gates, and in through a set of sliding metal doors. Tr. 43:15-44:20.

Once inside secondary, two other plain clothes officers were present at the search station as Officer Sottile began his search. Tr. 45:8-16. However, the uniformed officers in the room had their firearms visible. Tr. 28:7-17. An armed guard was stationed at the exit. Tr. 44:24-451; *see also* Government Exhibit 6. Again, Mr. Gavino was not free to leave. Tr. 45:5-7.

Officer Sottile conducted the search of Mr. Gavino's suitcase but recovered no contraband or money. Tr. 43:11-23. Instead of inquiring about Mr. Gavino's current reasons for travel Officer Sottile asked only "baseline questions" about Mr. Gavino's trip like "where did you – how was DR?" Tr. 52:24-53:4. He did not check to see if the items in his luggage were consistent with Mr. Gavino's explanation for travel. *See id.* In fact, there is no indication he ever asked Mr. Gavino the purpose of his trip. *See id.* He did not inquire about narcotics trafficking, possession of contraband, or anything about what Mr. Gavino had been doing in the Dominican Republic. *See id.*

Instead of engaging in this standard line of inquiry for secondary inspections, and despite finding no contraband, money, or other suspicious items in Mr. Gavino's luggage, Officer Sottile began to question Mr. Gavino about the 2019 stop in Texas. He claimed he found Mr. Gavino's answers to be suspicious, however, he admitted he did not know if the answers were consistent with the answers Mr. Gavino provided to law enforcement in 2019. Tr. 51:20-51:3. These answers to the 2019 stop were what lead him to search Mr. Gavino's phone. Tr. 52:12-23. Specifically, Officer Sottile testified "So I said, listen, let's call your friend so he can tell me what it was for. His response was, my friend died. I said, Can we call his brother? I don't talk to him any more, I don't have his number." Tr. 30:16-19. At that point Officer Sottile responded, "all right, you know what? You have your cell phone, let me see your cell phone" and began the search. Tr. 30:21-22; *see also* Tr. 52:8-13. When asked about why he looked at Mr. Gavino's

phone he initially stated "[b]ecause in the lookout it stated the approximately 37,000 was seized in 2019, and I believe it was for marijuana and the story he was giving me right now didn't make any sense. So I asked him to open the phone so I can verify what I suspected to be true." Tr. 32:6-12. He later claimed that while he wanted to search the phone for evidence related to "the 2019 incident…", that "would also show that he could be possibly doing that same activity now." Tr. 52:16-19.

Officer Sottile testified that in order to open the phone he first ordered Mr. Gavino to hand him the device. Tr. 32:13-14. This is inconsistent with the information he gave to Special Agent Shannon Christie that he "conducted a border search of Mr. Gavino's person and found the device." Tr. 81:15-23. He also claimed that after he obtained the device it was turned off and locked. Tr. 32:15-18. This again was contradicted by his prior statements where he said the "subject voluntarily presented the phone in a powered on and unlocked position" and never mentioned that he initially handed him the phone in a locked position. Tr. 53:19-55:22.

When Officer Sottile obtained the phone from Mr. Gavino it was locked. Tr. 32:15-18. He then asked Mr. Gavino to unlock it. Tr. 66:14-16. At first, Mr. Gavino refused and allegedly said, "can't you open it, you're the government?" Tr. 66:16-18. He then told Mr. Gavino that he could open his phone even if Mr. Gavino refused to provide his passcode, but that if Mr. Gavino refused, he would seize it and keep it for "months." Tr. 66:23-67:4.[2] While he did not know exactly what happens when a phone gets sent to a lab, he admitted that he believed it would be sent to a lab, opened, and an "*extraction"* would be performed. Tr. 67:12-68:18. This is

[2] This back and forth was not contained in the officer's case summary in the secondary inspection report. *See* Tr. 61:25-26:2. Nor did he mention that he had to charge and power on the phone at some time during the examination. *See* Tr. 66:7-13. Instead, the first time he made these claims was during a conversation with the AUSA in the fall of 2022 while preparing to respond to defense counsel's motion to dismiss based in part on Mr. Gavino's affidavit detailing what had occurred during the search. *See* Tr. 62:4-66:9.

consistent with his description of forensic searches. See Tr. 20:22-24. He claimed that after he obtained the phone in the unlocked position he asked for Mr. Gavino's passcode. Tr. 33:13-18.

While conducting the search he "looked through the text messages, photos. Initially, I didn't find anything in the text messages and I went to WhatsApp. In WhatsApp there was a contact named CP, I just opened it up and I found what appeared to be child pornography on the phone." Tr. 33:23-34:2. He claimed this search took only ten to fifteen minutes. Tr. 35:5-8. He later said it took only five minutes. Tr. 78:1. However, he admitted that during the search the device locked out multiple times and that he had to type in the passcode before finding any contraband. Tr. 37:1-14. The whole interaction and search took three-and-a half-hours. Tr. 68:23-67:6.

Officer Sottile testified that a "basic" or "manual" search could recover a lot of personal and private information including, for example: text messages, call logs, contacts, emails, calendars, photos, notes, and other private things. *See* Tr. 69:7-70:7. He also testified that a phone can contain essential things that you may need to live your daily life or even to leave an airport, including, for example: banking apps, passwords, phone numbers for friends and family, lift accounts etc. Tr. 70:8-71:3.

ARGUMENT

The manual search of Mr. Gavino's iPhone violated the Fifth and Fourth Amendments. *See* U.S. CONST. amends. V and IV. With respect to the Fifth Amendment violation, the requirement that Mr. Gavino unlock and decrypt his cell phone was compulsive, testimonial, and self-incriminating. Mr. Gavino was also forced to provide his passcode without first being advised of his *Miranda* rights. Under the Fourth Amendment, a warrant was required for the manual search, or at the least, the search should have been supported by reasonable suspicion or probable cause.

Accordingly, all evidence obtained from the manual search must be suppressed. Because the evidence obtained from the forensic search of Mr. Gavino's cell phone is the fruit of the initial search, that evidence must also be suppressed. Finally, because the statements Mr. Gavino made regarding what was found on his phone were a fruit of the initial search, his statements must also be suppressed.

I. Mr. Gavino was compelled to provide the passcode to his cell phone in violation of the Fifth Amendment.[3]

Mr. Gavino was compelled to provide his passcode when he was told that he could provide his passcode, or the police would seize his phone indefinitely (or at least for "several months") and search it without his consent. This demand threatened to remove property from Mr. Gavino that was essential to his everyday life and asserted authority which the officer did not have—the authority to conduct a forensic search of the device offsite.

Contrary to the government's assertions, the Court does not apply a voluntariness analysis to determine compulsion in the context of the compelled decryption of an electronic device. *See* Lawrence Rosenthal, *Compulsion*, 19 U. Pa. J. Const. L. 889, 891 (2017) (noting that there is no "workable definition" of compulsion and that the Court does not follow the dicta in *Washington*.); *see also Spevack v. Klein*, 385 U.S. 511, 514 (1967) (eschewing the "overborne will" analysis and instead noting the "right of a person to remain silent unless he chooses to speak in the unfettered exercise of his own will, and to suffer no penalty for such silence"); *Garrity v. New Jersey*, 385 U.S. 493, 504 (1967)(dissenting opinion) (noting the majority holding was not applying the overborne will test). Instead, courts look at whether government officials used their apparent (or real) authority or threats to obtain testimonial evidence. *See id.*

[3] With respect to the issue of the compelled decryption the defense here focuses only on whether the passcode was compelled as that was an issue of fact raised in the prosecution's motions. The testimony and incrimination prongs were addressed extensively in defense's prehearing motion. *See* ECF No. 22 at 6-8.

Mr. Gavino was compelled to provide his passcode because he was informed that his cooperation was unnecessary and that a refusal to provide the passcode would result in a deprivation of property. A person cannot have been said to have acted freely or voluntarily where they merely "acquiescence to a claim of lawful authority." *Bumper v North Carolina*, 391 U.S. 543, 549 (1968). This is because when law enforcement claims a right to search, "he announces in effect that the [target] has no right to resist the search. The situation is instinct with coercion -- albeit colorably lawful coercion. Where there is coercion, there cannot be consent." *Id.* at 550. This is especially true where the government claims authority that they do not have or where they use the threat of deprivation of personal property in order to obtain consent. *See United States v. Munoz*, 987 F. Supp. 2d 438 (S.D.N.Y. 2013); *United States v. Eggers*, 21 F. Supp. 2d 261, 269–71 (S.D.N.Y. 1998).

In *Munoz* the defendant was under arrest and police told his father they would get a search warrant for his apartment if he did not consent to a search. *Munoz*, 987 F. Supp. 2d at 446. However, police knew at the time that they lacked probable cause and therefore could not obtain a warrant under the law. *Id.* For that reason the court held that the consent was coerced. *Id.* at 447.

In *Eggers* the defendants were under arrest in their homes when federal agents informed them that if they consented to a search, their daughters would be allowed back into the house when they returned from school. *Eggers*, 21 F. Supp. 2d at 265. However, the agent informed them their daughters "would not be allowed back until a warranted search was conducted, perhaps not for several days if consent was refused." *Id.* One of the key factors that the court used in finding the consent was involuntary was this threat to prohibit the defendant's school age daughters from reentering the property. *Id.* at 270. The court also noted that at the time the threat was made agents were not sure if they would or even could obtain a warrant. *Id.* n.80.

Similarly, Officer Sottile claimed a right to search the phone using a forensic extraction. Specifically, he told Mr. Gavino that if he did not provide his passcode, he would send it to a lab and unlock it without Mr. Gavino's assistance. He understood this to mean he would conduct a forensic search of the device by sending it to a lab for an "extraction" or a "forensic" or "advanced" search rather than a "basic" or "manual" search.[4] However, he had no authority to conduct a "forensic" search under existing appellate law or the internal rules of the CBP. *See e.g. United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019); *Border Search of Electronic Devices* CBP Directive No 3340-049A § *5.1.4.* The CBP rules only allow a "forensic search" where there is "reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern… an Officer may perform an advanced search of an electronic device." *See id.* At that point in time Officer Sottile did not have reasonable suspicion to search the device. S*ee infra* § III (B).

Furthermore, Officer Sottile's threat to deprive Mr. Gavino of his property also compelled him to provide his passcode. As Officer Sottile acknowledged on cross examination, a phone can contain essential things that people need to live their daily lives or even to leave an airport including, for example: banking apps, passwords, phone numbers for friends and family, lift accounts etc. Telling Mr. Gavino he would lose access to those things was a threat to deprive him not only of essential property, but his means of communication, transportation from the airport, and daily necessities.

Mr. Gavino did not voluntarily or consensually provide his passcode to Officer Sottile. Instead, he was coerced into providing the passcode by threats to confiscate essential property for

[4] He admitted that the lab would "extract the data" from the phone at the lab. Tr. 68:10-18. An extraction is the copying of the contents of a device. *See* privacyinternational.com, A technical look at Phone Extraction, at 4-6, https://privacyinternational.org/sites/default/files/2019-10/A%20technical%20look%20at%20Phone%20Extraction%20FINAL.pdf (last visited August 22, 2023).

"months" and by claims of authority that Officer Sottile did not have. Therefore, the passcode was compelled.

II. Mr. Gavino was in custody when he was compelled to provide his passcode.

Forcing Mr. Gavino to provide his passcode further violated the Fifth Amendment because he was in custody and had not been *Mirandized* when he was compelled to provide his passcode. While the prosecution analogizes this case to FNU LNU and other common border search cases, the facts of this case are distinguishable and instead analogous to an Eastern District of New York case, *United States v. Djibo*, 151 F. Supp. 3d 297 (E.D.N.Y. 2015), because here as in *Djibo*, obtaining his passcode "had nothing to do with national security at the airport on that day." *Id.* at 310.

In *Djibo*, the defendant was being investigated for heroin trafficking when law enforcement received intelligence that he would be traveling by air from the United States to London. *Id.* at 298–99. Law enforcement agents targeted Djibo for a "border search" and seized, *inter alia*, his iPhone 5. *Id.* at 299. The agents then asked Djibo for his passcode, which he provided. *Id.* The agents purported to do a "basic "search of the phone at that time to look for evidence of currency or other illegal activity. *Id.* at 302. A month later, the agents obtained a search warrant to conduct a forensic search. *Id.* The court held that the statement identifying the passcode to Djibo's iPhone was suppressible under the Fifth Amendment, *id.* at 306, and that evidence from the subsequent, warrant-supported forensic search was suppressible as its fruit. *Id.* at 310.

In *Djibo* the court found that despite the fact he was flying internationally three factors lead them to conclude that *Djibo* was in fact in custody at the time he provided his passcode. *Id.* at 306. First, he was not free to leave once he was asked to step aside "to a private area" for currency exam. *Id.* Second, a Homeland Security ("HIS") agent was present during the search. *Id.* Third, no

contraband was found in his luggage and the border search was essentially over. *Id.* The court also noted "the line of inquiry into Djibo's telephones thereafter completely changed the stage because the purpose of the original search was to find currency and currency cannot be found on a phone." *Id.* The court also went on to distinguish *FNU LNU*, explaining that in that case, the agents were properly questioning her about a key aspect of border security - her identity. *Id.* They also noted that the Second Circuit in *FNU LNU* commented that "'[p]ractically speaking, the *most* important factor in determining whether *Miranda* applies at our borders will often be the objective function of the questioning.'" *Id.* (citing *United States v. FNU LNU*, 653 F.3d 144, 155 (2d Cir.2011)).

Here, Mr. Gavino was pulled from primary inspection and escorted to pick up his bags by Officer Sottile who was wearing a badge and introduced himself as a federal law enforcement officer. Officer Sottile testified that Mr. Gavino was not free to leave that point. Officer Sottile then escorted Mr. Gavino past exit signs and away from where other travelers were going. Officer Sottile brought Mr. Gavino through a set of metal gates and sliding doors. Three plain clothes officers were present during the search of his luggage while other uniformed armed officers remained in the room with one stationed at the exit. Again, Officer Sottile testified Mr. Gavino was not free to leave. Given his surroundings, that fact would have been very apparent to Mr. Gavino. Furthermore, the questions asked of Mr. Gavino had nothing to do with his current trip. Instead, Officer Sottile interrogated him about an incident from two years prior where the government had taken $37,000 from Mr. Gavino. Therefore, like the defendant in *Djibo*, he was not free to leave. In fact, he was in a far more restrictive area surrounded by officers (some of them armed). He was also being questioned about a prior domestic incident and not his current international travel. The objective functioning of these questions was not therefore border related but rather it was an interrogation about a past crime. This is further supported by the fact the officer

asked to search his phone immediately after he stated he did not have the phone number of his friend's brother. Therefore, like the defendant in *Djibo*, Mr. Gavino was in custody for the purposes of *Miranda*.

III. The warrantless manual search of Mr. Gavino's phone violated the Fourth Amendment where it was conducted to look for evidence of a past crime rather than contraband.

The manual search of Mr. Gavino's phone violated the Fourth Amendment by infringing upon the expansive privacy interests inherent within his digital device.

A. A warrant is required to conduct a manual search of a modern smartphone for evidence of a crime.

While there is longstanding doctrine allowing suspicionless border searches of one's person and luggage for physical contraband, the Supreme Court has warned against "mechanical" application of old doctrine to new technologies like cellphones. *Carpenter v. United States*, 138 S.Ct. 2206 (2018) (*quoting Kyllo*, 533 U.S. at 35); *see also Riley*, 573 U.S. at 393 (rejecting application of the search incident to arrest doctrine to cell phones found in an arrestee's possession). For this reason, one court in the Southern District of New York recently held that a warrant was required to perform a search of an electronic device at the border where the search was not targeting contraband, but evidence of past and ongoing crimes. *See United States v. Smith*, 2023 WL 3358357 (S.D.N.Y. 2023).

Before *Smith* was decided, the Fourth Circuit addressed the issue of whether the border search doctrine covered searches of electronic devices where the government only had reason to believe the traveler had committed domestic crimes. *See United States v. Aigbekaen*, 943 F.3d 713, (4th Cir. 2019). In that case, Aigbekaen was accused of trafficking a minor using Backpage.com and transporting her "around Maryland, Virginia, and Long Island, New York." *Id.* at 717. When HSI agents learned that Aigbekaen was returning to the United States through John F. Kennedy

Airport they asked CBP officers to seize his devices. *Id.* at 718. CBP "honored this request and, without warrants, seized Aigbekaen's MacBook Pro laptop computer, iPhone, and iPod." *Id.*

The court noted that the government had "not only reasonable suspicion but probable cause to believe the suspect had previously committed grave *domestic* crimes." *Id.* at 721. However, the court held the searches for evidence of a domestic crime "lacked the requisite nexus to the recognized historic rationales justifying the border search exception." *Id.* The court rejected the government's argument that the nexus existed merely because "'[sex trafficking] is a crime 'commonly involving cross-border movements.'" *Id.* Instead they required the government to offer some "reasonable basis to suspect that Aigbekaen's domestic crimes had any such transnational component…" before invoking the border search exception. *Id.* For those reasons, the court held that the warrantless forensic search did not fit into the border search exception and violated the Fourth Amendment.

In *Smith*, HSI and the Federal Bureau of Investigations ("FBI") were investigating a conspiracy to control the New York area emergency mitigation services ("EMS") industry. *Id.* at *2. The FBI and HSI requested that CBP stop and search Smith pursuant to their border authority. *Id.* When reentering the country at Newark airport, police seized his phone, obtained his passcode, and made a forensic copy of the phone. *Id.* at *3. They conducted a search of the device and recovered incriminating data. *Id.*

The court, following the direction of the Supreme Court in *Riley*, "analyzed whether the logic behind the warrant exception [for searches at the border] applied to cell phone searches." *Id.* at *5 (citing *Riley*, 573 US at 373). In so doing, the court found that "[n]one of the rationales supporting the border search exception justifies applying it to searches of digital information contained on a traveler's cell phone, and the magnitude of the privacy invasion caused by such

searches dwarfs that historically posed by border searches and would allow the Government to extend its border search authority well beyond the border itself." *Id.* at *7. The court noted that the government's interest in the border search exception include things like apprehending persons who pose a threat or who lack authorization to be in the country, inspect goods to ensure taxes are paid, and prevent harmful goods like contraband or disease from entering the country. *Id.* The court then explained that the nature of data on a smartphone is different in that it rarely exists just on the phone itself, but in the cloud on servers around the world. *Id.* at *8. Therefore "[s]topping the cell phone from entering the country would not… mean stopping the data contained on it from entering the country." *Id.* The court weighed the "relatively weak governmental interest" against a citizen's privacy interests in her cell phone which "likely contains huge quantities of highly sensitive information -- including copies of that person's past communications, records of their physical movements, potential transaction histories, Internet browsing histories, medical details, and more." *Id.* In so doing, the court held, consistent with *Riley*, a warrant is required for a border search of an electronic device. *Id.*

Other courts have similarly rejected mechanical application of the border search rules where the search was conducted to locate evidence of a crime rather than contraband. *See Cano*, 934 F.3d at 1002 (requiring the government have reasonable suspicion that *contraband* exists on a device); *see also United States v. Kim*, 103 F.Supp.3d 32, 45 (2015)(engaging in a balancing test where the search was for evidence of a crime not contraband); *United States v. Djibo*, 151 F.Supp.3d 297 (E.D.N.Y. 2015)(finding that obtaining a passcode in order to conduct search of a device after no physical contraband or currency was recovered "cannot be considered within the purview of a border search.").

Notably the court in *Smith* did not distinguish between a "manual" or "basic" search and an "advanced" or "forensic search." This again is consistent with *Riley*, which required a warrant for "manual" searches of a device. *See Riley*, 573 U.S. at 379-380. Furthermore, this distinction between so called "manual" and "forensic" searches makes little sense in the Fourth Amendment context. *See United States v. Kim*, 103 F.Supp.3d 32, 45 (2015) (noting that whether a search of a device is "reasonable under the Fourth Amendment… does not turn on the application of an undefined term like "forensic."). While forensic searches can, in some instances, obtain things like metadata and deleted data that is not viewable during a manual search, some "forensic" searches like a "logical" imaging obtain the same data you would see in a "manual search."[5] However, the types of data that the Supreme Court considers the "privacies of life" are our photographs, notes, bank statements, calendars and other things that can be discovered in a "manual search." *See Riley*, 573 U.S. at 394; *see also* Tr. 69:7-70:7 (discussing manual searches). Finally, this distinction between "manual" and "forensic" arose from *United States v. Cotterman*, 709 F.3d 952 (2013), a decision which predates *Riley* and a search which predates modern smartphones.[6] As a result, the *Cotterman* decision failed to adequately discuss the privacy concerns implicated by searches of modern smartphones and draws a false distinction between the invasiveness of a "manual" and "forensic" search.

Here, CBP was searching for evidence of a past domestic crime - the possession of $37,000 in 2019 and Officer Sottile's belief that Mr. Gavino was using that money to purchase marijuana. When asked about why he looked at Mr. Gavino's phone he initially stated "[b]ecause

[5] *See* privacyinternational.com, A technical look at Phone Extraction, at 4-6, https://privacyinternational.org/sites/default/files/2019-10/A%20technical%20look%20at%20Phone%20Extraction%20FINAL.pdf (last visited August 22, 2023).
[6] *Riley* was decided on June 25, 2014, while *Cotterman* was decided on March 8, 2013. The Search in *Cotterman* was conducted on April 6, 2014, while the first-generation iPhone was released on June 29, 2007. *See* https://en.wikipedia.org/wiki/IPhone_(1st_generation) (last visited August 22, 2023).

in the lookout it stated the approximately 37,000 was seized in 2019, and I believe it was for marijuana and the story he was giving me right now didn't make any sense. So, I asked him to open the phone so I can verify what I suspected to be true." Tr. 32:8-12. This is consistent with Officer Sottile's testimony that after Mr. Gavino stated he did not have his friend's brothers phone number, Officer Sottile responded, "all right, you know what? You have your cell phone, let me see your cellphone" and began the search. Tr. 30:21-22.

While it is true that Officer Sottile later claimed that the search "would also show that he could be possibly doing that same activity now," the mere fact that a crime (like drug trafficking) commonly involves cross-border movements does not absolve the government of providing some individualized suspicion that the individual searched was involved in an international crime. Tr. 52:18-19. Officer Sottile's speculation that Mr. Gavino was involved in international drug trafficking because he was coming from the Dominican Republic and previously had $37,000 on a domestic flight is insufficient. Furthermore, Officer Sottile's post hoc justification for the search is belied by his actions on scene. He testified that the purpose of a secondary inspection is to "to examine the person that travels, what they stated they went there for and to conclude that it was legitimate travel, you have a legitimate traveler in front of you." Tr. 10:9-12. Officers are supposed to "ask [travelers] about their bags, if its's theirs, they packed it." Tr.10:20-25. They are supposed to search luggage to "make sure [no contraband] comes into this country" and that their luggage "matches" their travel. Tr. 10:16-17. He explained "[s]ome people say they're going for a wedding, you're going to look for a dress, a suit. Something that matches their travels. If they're going for vacation, they're going to the beach, you're going to look for swimming trunks and T-shirts. Generally it's to match what they're saying they traveled for." Tr. 18:1-7. However, during his interaction with Mr. Gavino he did none of these things.

Instead of inquiring about Mr. Gavino's reasons for travel to the Dominican Republic, Officer Sottile asked only "baseline questions" about Mr. Gavino's trip like "where did you – how was DR?" Tr. 53:2-4. He did not check to see if the items in his luggage were consistent with Mr. Gavino's explanation for travel. In fact, there is no indication he ever asked Mr. Gavino about the purpose of his trip. He did not inquire about narcotics trafficking, possession of contraband, or anything about what Mr. Gavino had been doing in the Dominican Republic. Instead, the entire focus of his questioning was about the 2019 stop.

Here Officer Sottile neither obtained a warrant nor had probable cause before searching Mr. Gavino's phone. *See infra* § B (discussing reasonable suspicion). Therefore, the contents of the iPhone and any fruits obtained therefrom must be suppressed.

B. The search of Mr. Gavino's iPhone was not supported by reasonable suspicion.

Even if this Court were to apply a lesser standard of reasonable suspicion, suppression would be required in this matter because Officer Sottile had no reason to believe Mr. Gavino was committing any ongoing crimes or smuggling contraband. Instead, Officer Sottile's search of Mr. Gavino's device was a fishing expedition for information from the 2019 stop and other possible narcotics activity.

Several courts have suggested reasonable suspicion is required to search a device at the border.[7] *See e.g. Cano*, 934 F.3d at 1002; *see also United States v. Kolsuz*, 890 F.3d 133, 137 (4th Cir. 2018), *as amended* (May 18, 2018) (requiring "some level of individualized suspicion"); *contra Alasaad v. Mayorkas* (1st Cir. 2021); *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018) "[T]he reasonable suspicion standard relates to ongoing or imminent crime." *Kim*, 103 F.Supp.3d

[7] Again, the distinction between "manual" or "basic" and "forensic" searches is often a distinction without a difference and is misplaced. See supra. at p. 16-17. Therefore, that aspect of the reasonable suspicion cases is not discussed here.

at 45 (citations omitted). Therefore, "evidence of prior criminal conduct alone is not sufficient to give rise to reasonable suspicion." *Id.* In *Kim*, HSI was investigating a man named Bin Yang for export violations. *Id.* at 35. Yang was arrested and while in custody in 2012 told investigators that four years prior Kim had shipped six accelerometers to him in China without an export license which Yang then sold to Iranian customers. *Id.* at 37. Based on that information the case agent decided to conduct a border search of Kim at LAX on December 5, 2012. *Id.* at 39. First, the agent checked Kim's luggage and found no accelerometers or other evidence of illegal exports. *Id.* Despite having no evidence of any ongoing crimes or that any crime was afoot he stopped Kim and seized his electronic devices. *Id.* at 40. During the hearing the agent explained that he believed, based on Yang's statements, that Kim might be involved in other illegal export activity and that his devices might have evidence of the 2008 transactions. *Id.* at 38.

The court rejected the government's claims that the case agent had reasonable suspicion to search the devices. *Id.* at 43-49.[8] The court noted that "while it is a close case, it seems clear to the Court that the search of the laptop was predicated upon the agent's expectation that the computer would contain evidence of past criminal activity, but there was no objective manifestation that Kim was or was 'about to be, engaged in criminal activity' at that time. With respect to ongoing activity, the search was nothing more than a fishing expedition to discover what Kim might have been up to." *Id.* at 46 (citations omitted). They noted the agent had no information "where Kim had gone during his trip or who he contacted during his travels." *Id.* at 49.

Here, it is apparent that Officer Sottile was merely engaged in a fishing expedition to search for evidence of past crimes and other general ongoing activity affecting the border. All that Officer

[8] Despite examining the issue of reasonable suspicion, the court in *Kim* refused to fully apply the reasonable suspicion standard because the search could not "be fairly compared to a Terry stop." *Id.* Instead, the court applied a balancing test and found the search unconstitutional suppressing the contents of the devices. *Id.* at 49-59.

Sottile knew about Mr. Gavino was that in 2019 he had been stopped in Texas while on his way to a domestic flight to LAX and approximately $37,000 had been seized from him. He knew that Mr. Gavino was never arrested or charged with a crime and that no drugs or contraband was recovered. He was not aware of any incidents since 2019. Therefore, unlike the agent in *Kim,* he had no probable cause to believe Mr. Gavino had committed a crime in the past. More importantly, Officer Sottile knew nothing about Mr. Gavino's travels on August 30, 2021, other than the fact he was coming from the Dominican Republic to New York. Despite his dearth of information about Mr. Gavino and his travels, he believed that Mr. Gavino was involved in marijuana and narcotics trafficking. Based on nothing more than these suspicions he searched Mr. Gavino's bag and interrogated him about the 2019 stop. When Mr. Gavino provided answers to his interrogation that he believed were unsatisfactory, he searched Mr. Gavino's phone by looking at text messages, photos and possibly other parts of the phone before searching his WhatsApp application. It was only after scrolling through all of those other areas for long enough that he had to enter the password multiple times that he discovered the contraband at issue in this case.

The 9th Circuit applies an even stricter standard—requiring not just proof of an ongoing or imminent crime, but reasonable suspicion that contraband is present in the electronic device searched. *Cano*, 934 F.3d at 1007. If that standard were applied here suppression would clearly be mandated. Officer Sottile did not provide any testimony that would allow him to infer there was any contraband on the device at the time he searched it. Instead, his investigation into Mr. Gavino's phone was based on his idea that because Mr. Gavino once had $37,000 on him while on a domestic flight, and was coming from the Dominican Republic, he might be currently engaged in drug trafficking. Therefore, the police lacked the necessary suspicion to search his phone.

IV. The Good Faith Doctrine does not apply here because the only binding caselaw on the subject of device searches was *Riley*.

The government claims that suppression is not warranted under the good faith doctrine. However, the good faith exception does not apply where the warrant was issued on the basis of evidence unconstitutionally obtained and where the exclusion of the evidence would alter the behavior of law enforcement. *See United States v. Reilly*, 76 F.3d 1271 (2d Cir. 1996); *see also* ECF 27 at 12-15. Furthermore, the government failed to establish that Officer Sottile's pre-warrant actions relied in good faith on binding appellate precedent as is required by the Second Circuit. *United States v. Aguiar*, 737 F.3d 251, 262 (2d Cir. 2013).

The government cannot rely in good faith on the warrant because the warrant was obtained through the use of evidence obtained in violation of the law. *See United States v. Reilly*, 76 F.3d 1271, 1281 (2d Cir. 1996). It is of no moment that the officers seeking a warrant are different from those who committed the initial constitutional violation. *See e.g. United States v. McGough*, 412 F.3d 1232, 1235 (11th Cir. 2005) (officer who engaged in the initial unlawful entry did not obtain the warrant); *State v. Reno*, 260 Kan. 117, 119 (Kan. 1996) (undersheriff—not the deputy sheriff conducting the illegal entry—obtained two search warrants); *McGinnis v. United States*, 227 F.2d 598, 603 (1st Cir. 1955) (federal agents participating in an unlawful state search pursuant to a unparticularized warrant cannot subsequently avoid suppression by obtaining a properly particularized federal warrant); *cf. United States. v. Burgard*, 675 F.3d 1029 (7th Cir. 2012) (both federal and local law enforcement responsible for the six-day delay in obtaining a warrant). Just as "[p]olice officers cannot launder their prior unconstitutional behavior by presenting the fruits of it to a magistrate…" *State v. Hicks*, 707 P.2d 331, 333 (Ariz. Ct. App. 1985), neither can they launder the prior unconstitutional behavior of their fellow officers. *See Franks*, 438 U.S. at 163 n.6 (recognizing that police cannot "insulate one officer's deliberate misstatement merely by relaying it through an officer-affiant personally ignorant of its falsity").

The government conflates good faith reliance on a warrant and good faith reliance on binding appellate precedent. See ECF 25 at 27 *citing United States v. Raymonda*, 780 F.3.d 105, 119 (2d Cir. 2015). The court in *Raymonda* held only that a prior holding by a district court could not establish a binding principle that undermines an agent's good faith reliance on ***a warrant***, not good faith reliance on non-binding caselaw. *Id.* at 118. The reference to the reliance on a district court case was simply to point out that a single district court case with a somewhat similar fact pattern did not fall under the third *Leon* exception for situations where "the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable." *Id.*

Objective reliance on the law requires that the government actions are supported by binding appellate precedent. *Davis v. United States*, 564 U.S. 229 (2011); *Aguiar*, 737 F.3d at 251. The Second Circuit in *Aguiar* explained "'binding precedent' refers to the precedent of this Circuit and the Supreme Court." *Id.* at 261. The court rejected the idea that police could rely on non-binding caselaw from other circuits. *Id.* When it came to binding precedent the court required an analysis of the underlying principles of the existing caselaw as well as a comparison between the facts of the cases. *See id.*

The court in *Smith* reasoned that the Second Circuit's decision in *Levy* was factually similar enough to allow an officer to rely on it in good faith to search an electronic device. *Smith*, 2023 WL 3358357 at *14 (citing *United States v. Levy*, 803 F.3d 120 (2d Cir. 2015)) However, *Levy* involved a search of a book not an electronic device and predated *Riley*. *See Levy*, 803 F.3d at 120. Since *Levy* was decided and before the search at issue in this case, the Supreme Court made it clear that a phone is nothing like a notebook. *See Riley v. California*, 573 U.S. 373, 393 (2014). "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." *Id.* They are "cameras, video players, rolodexes, calendars, tape recorders,

libraries, diaries, albums, televisions, maps, or newspapers." *Id.* "[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record." *Id.* "Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house." *Id.* at 396. Comparing a notebook to a cellphone is like comparing a ride on horseback to a flight to the moon "[b]oth are ways of getting from point A to point B, but little else justifies lumping them together." *Id.* Therefore, unlike in *Aguiar* the act of searching a phone is not "nearly identical conduct to that authorized in [*Levy*]." *United States v. Katzin*, 769 F.3d 163 at 175 (3d Cir. 2014) (stating that the use of a GPS device in that case was "nearly identical conduct to that authorized in *Knotts*."). Instead, the binding precedent as it relates to device searches is *Riley* which clearly indicates that a warrant is required for a "basic" or "manual" search.

Furthermore, the question of whether the good faith doctrine applies in this situation has already been answered by the Ninth Circuit which held:

> We understand that border officials might have thought that their actions were reasonable, and we recognize that border officials have to make in-the-moment decisions about how to conduct their business—whether or not they have written guidance from the courts. But as we understand the *Davis* rule, the good faith exception to the exclusionary rule applies only when the officials have relied on *binding* appellate precedent. This is a rapidly developing area, not an area of settled law.

Cano, 934 F.3d at 1022 (declining to apply the good faith exception to the unconstitutional manual and forensic border searches of a cell phone).

Also, even if the Court finds that there was good faith given the lack of binding decisions on device searches at the border, there is no good faith exception for the compelled decryption or *Miranda* violations.

CONCLUSION

For all of the aforementioned reasons, the manual search of Mr. Gavino's iPhone 11 violated the Fifth and Fourth Amendments. All evidence seized from the cell phone and any fruits thereof, including statement evidence and evidence from the subsequent forensic search, must be suppressed.

Respectfully submitted,

ALEXEY RENE GAVINO

By: _____/s/_____
Marissa Sherman
Sidney Thaxter
Attorneys for Alexey Rene Gavino